Virginia Information Technologies Agency

Architecture Overview

Agency Acronym – Application Title

Version 1.0

www.vita.virginia.gov

Architecture Template Revision: 2.3 as of 10/1/19

Instructions for this Template:

Text in blue is help or example data – please delete it before turning in your Architecture. . Also all diagrams are examples.

Note: all diagrams are in embedded Visio Diagrams

Revision History

Date	Author	Version	Change reference

Date of next review: _____

<this is one year after the approval>

Contents

1. Purpose

1.1 Application Purpose

<This is the description of why you are deploying this application>

1.2 Solution Component Overview

<This is where vendor marketing info should be used to answer the below questions.

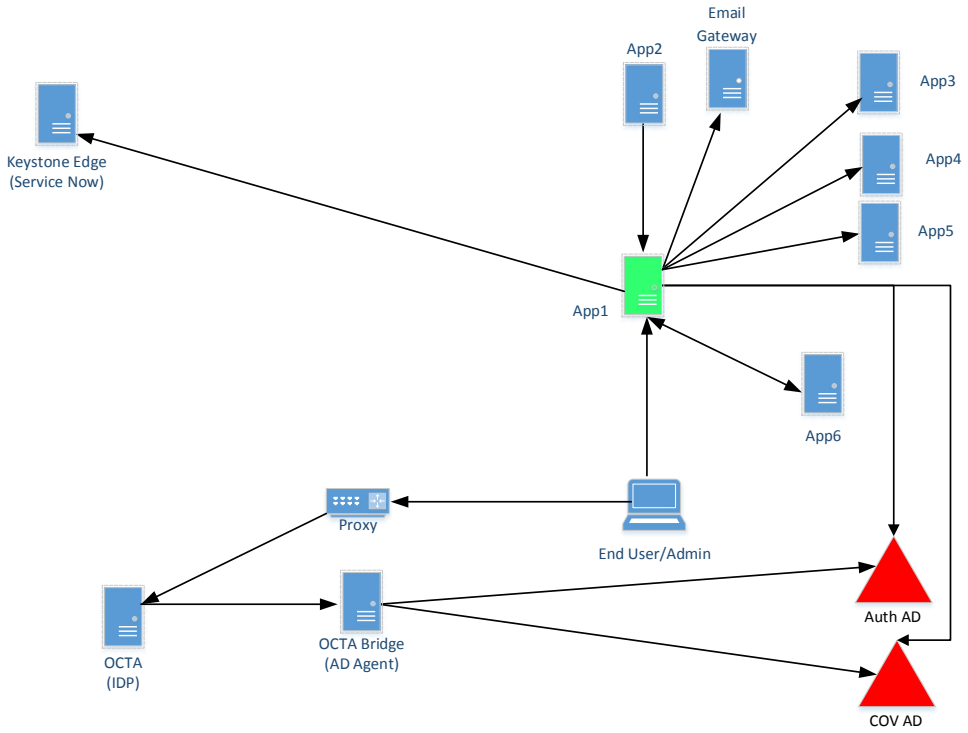
- What is it
- What business requirements are you solving for
- Features
- Benefits
- How it works
- Other possible Business Requirements it might be able to solve >

2. Context

2.1 System Interactions

Application Logical Layer Drawing

<this is an overall, high level drawing of how your system interacts/communicates to other systems.>

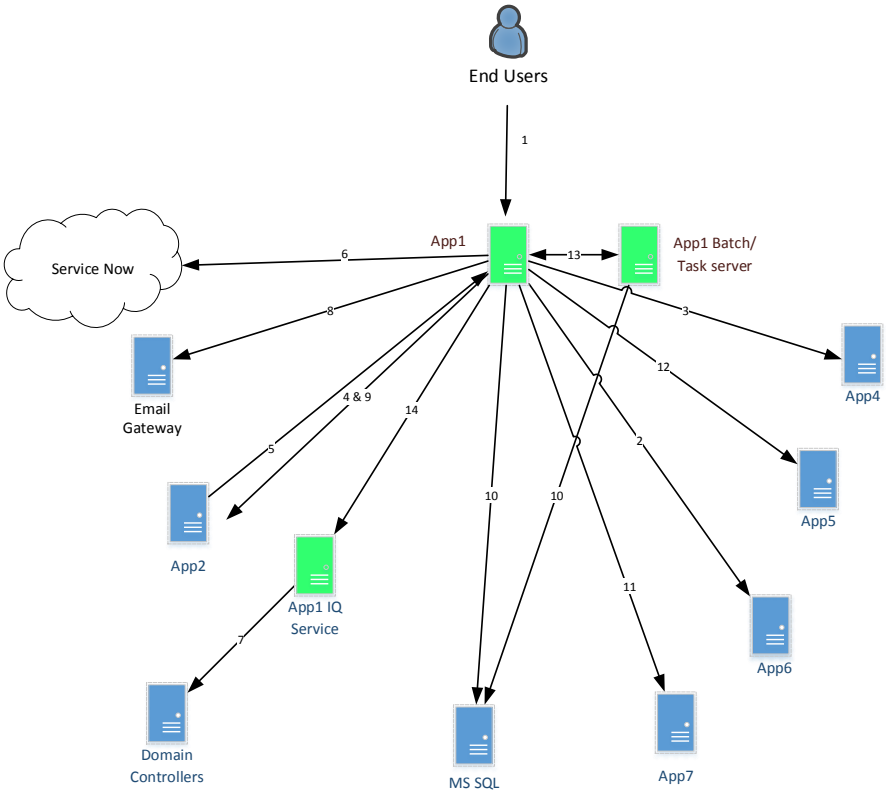


Application Communications Drawing

<Must include

- All systems that your application is communicating with
- All ports being used
- Communication direction between systems – if bidirectional you need 2 lines and 2 rows in the Ports table.
- Delineate between which systems are in your application and which are not
  - Easiest to color them differently
- Number the paths of communication
- Drawings and the ports tables must match
- Make sure that all communications listed in the text body of this document are listed
  - Such as systems you are dependent on and systems that will depend upon you.

SailPoint – Port View



Interface Descriptions

3.Interface Descriptions

Name and Number	Description	Source (from)	Target (to)	Port and Protocol	Is it Batch?	Fill in only if batch: How often	Fill in only if batch: size	Fill in only if batch: File type	Interface Disposition (reuse, new, updated)	Scope (not shared, multi-agency or Commonwealth
1	Web Access Interface	End-user	App1	TCP/443 HTTPS	N				New	Commonwealth
2	App6	App6	App1	TCP/5989 WBEM	N				New	Commonwealth
3	App4	App1	App4	TLS/514, TCP/9997 App4	N				New	Commonwealth
4	App2 Interface 2	App1	App2	TCP/1858 App2	N				New	Commonwealth
5	App2 Interface 3	PSM	App1	TCP/3389 RDP	N				New	Commonwealth
6	Service Now Interface	App1	Service Now Cloud	TCP/443, TCP/5989, HTTPS	N				New	Commonwealth

7	AD Communication	App1	Domain Controllers	TCP/636 LDAPS	N				New	Commonwealth
8	Email Gateway Interface	App1	Email Gateway	TCP/25 SMTP	N				New	Commonwealth
9	App2 Interface 3	App1	App2	TCP/8050 SCIM	N				New	Commonwealth
10	DB Access	App1	SQL DB	TCP/50000 SQL	N				New	Commonwealth
11	App7	App1	vRealize	TCP/5989 WBEM	N				New	Commonwealth
12	App5	App1	Digital Fuel	TCP/5989 WBEM	N				New	Commonwealth
13	App1 Batch	Batch Server	App1	TCP/8260 App1	N				New	Commonwealth
14	App1 IQ Servers	App1	App1 IQ Servers	TCP/5989 WBEM	N				New	Commonwealth

<Listing of preferred ports:

Encrypted Communications – Preferably authenticated via certificates on both sides

LDAPS – TCP/636 or TCP389 over TLS – No clear text 389

HTTPS - TCP/443

SQL – one port of TCP/50000 - 500100

SNMP v3

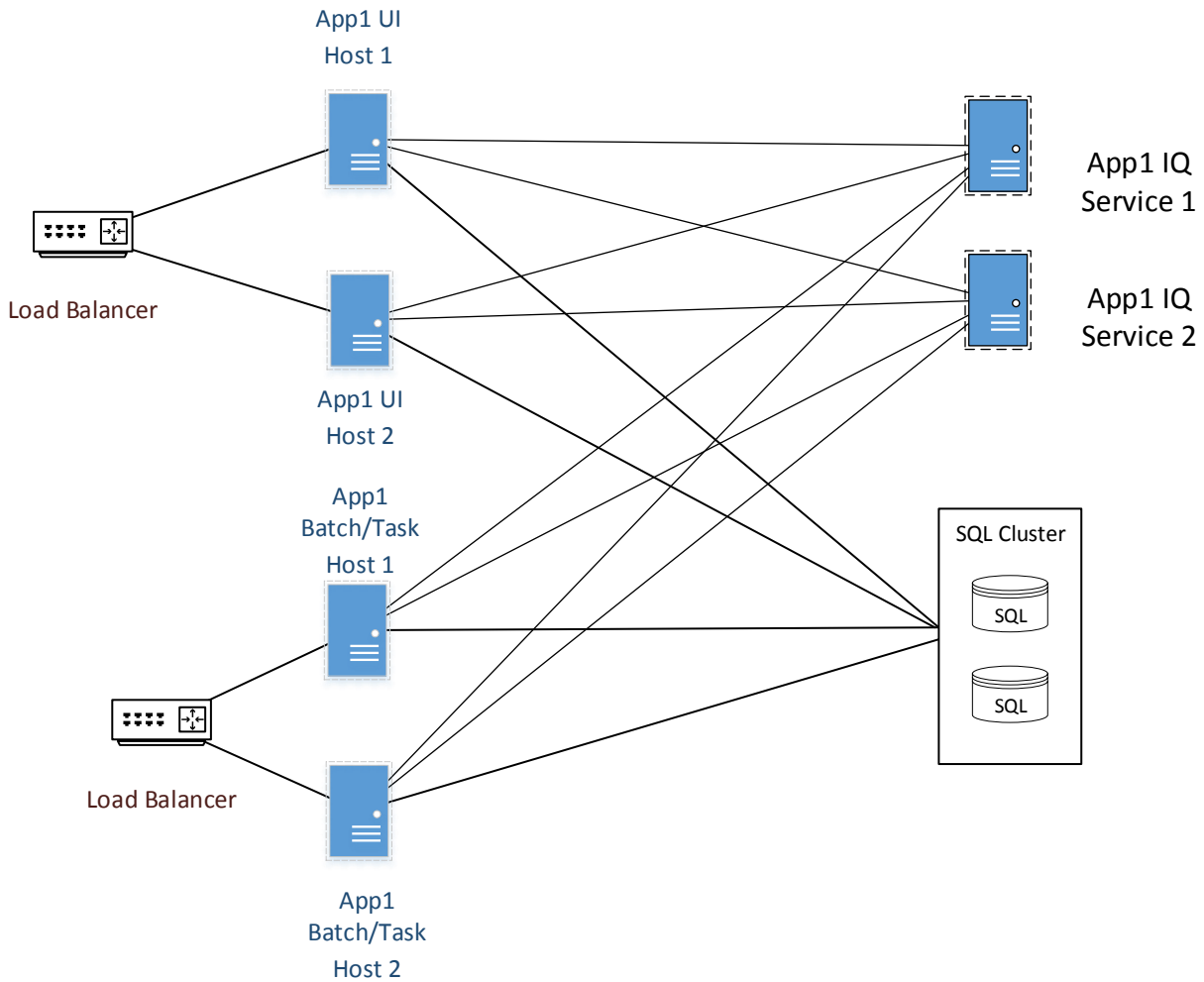
4.Operational Model

<This represents all systems you need to run. A diagram per environment – production, test, development and disaster recovery - Include load-balancers, firewalls, etc.>

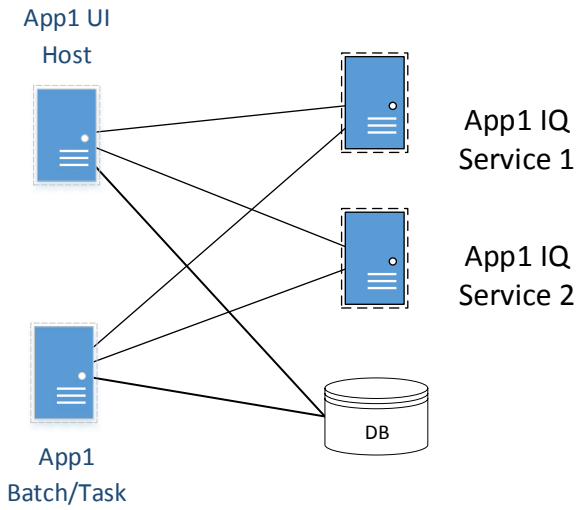
4.1 Resiliency Diagrams

<Required if it impacts more than one agency>

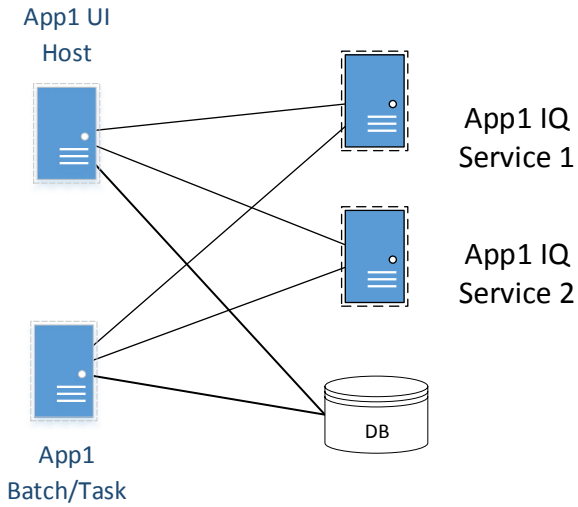
Production



Test



Development



Disaster Recovery

<needs to detail RTO and RPO and how they are being accomplished.>

For App1 we need:

1) 6 Servers (cold) with the patched software version that is in production

2) 2 SQL Clusters (warm) replicated from production (log shipping)

3) Setup the data sources (servers or applications to your application)

4) RTO = _____

5) RPO = _____

6) Backup Location:_____

7) Backup retention time: _____

5. Security Domain Model

5.1 Network Security Diagram

<this is where you put the Network security area you system is located – the Yellow lines are firewalls. These are the Predefined Security Buckets your component lives in

Internet – This is outside any control of the Commonwealth

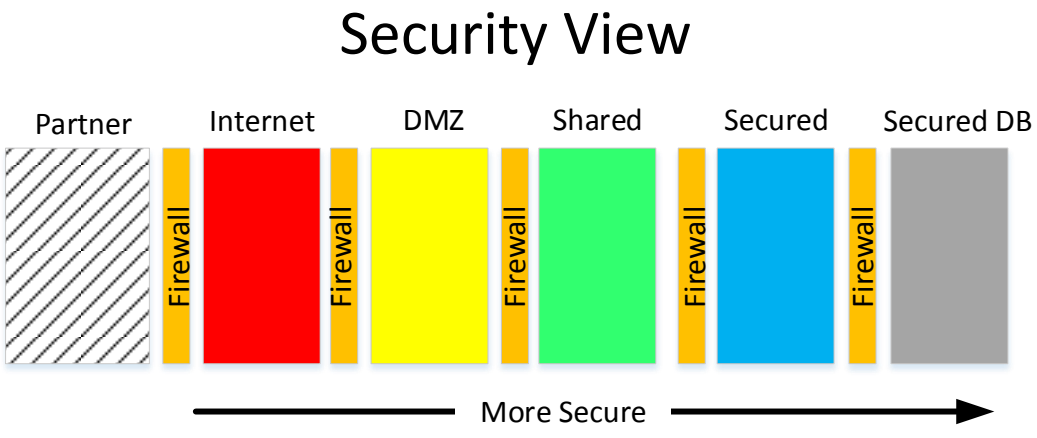
DMZ – This is the area where devices that must have incoming access from the internet live

Shared – Open to all internal users

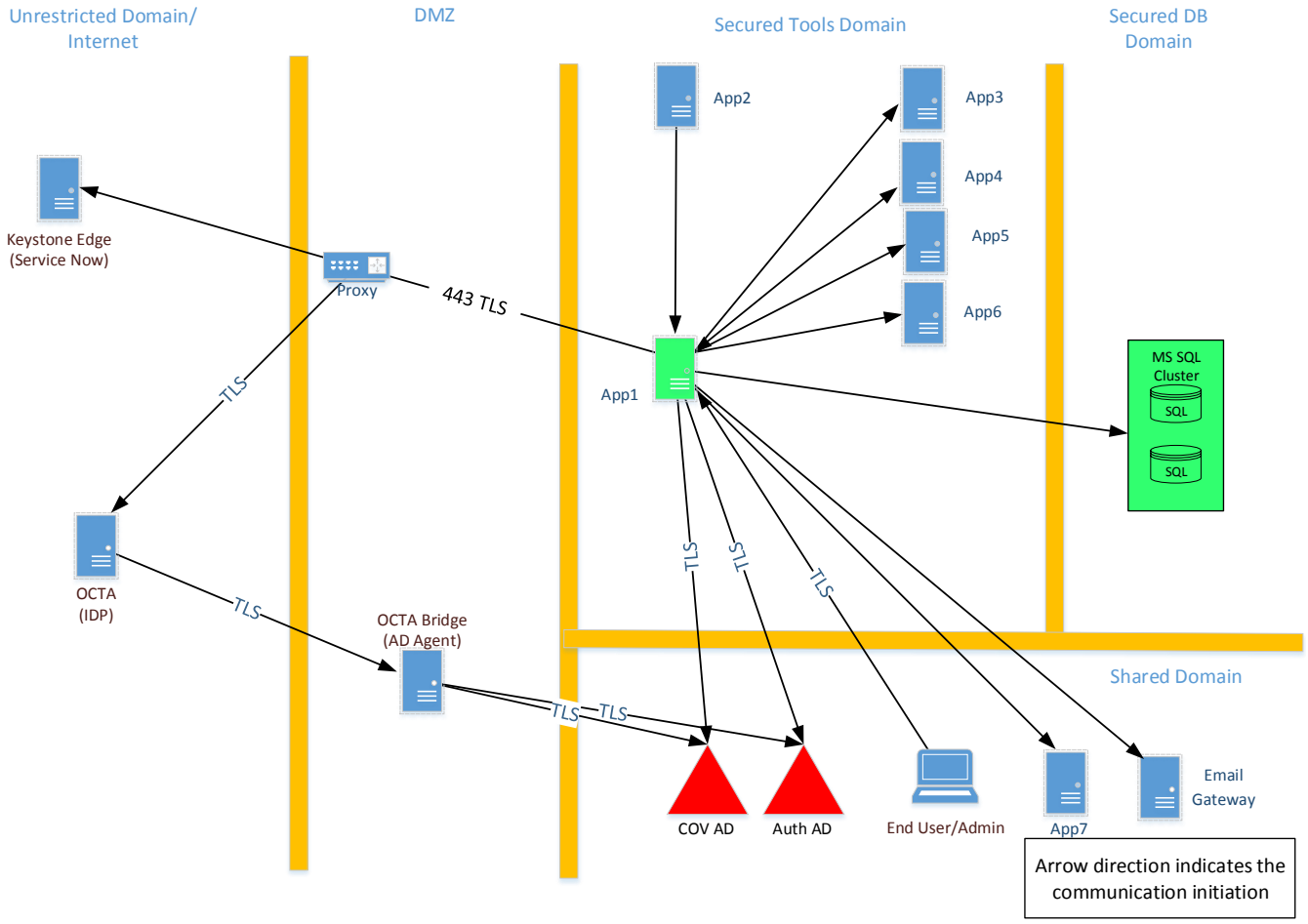
Secure – sensitive data and systems must exist in here

DB Secure – DB's not on a server, must live in a separate secure security domain

Partner – this where a secure, dedicated path to systems across the internet >



Architecture Overview



User Identity Source

<This is where your users are>

☐ AD

☐ External _____

☐ Other _____

Authentication source

<Where is the authentication source/method>

☐ AD

☐ Okta (SAML)

☐ SLDAP

☐ Local – Justify

_____

Authorization source

<Where is the authorization source/method>

☐ **Active Directory** Domain _____<COV, AUTH, etc.>

☐ **Groups**

<List them here> _____

☐ **Attributes**

<List them here> _____

☐ **SLDAP** Database name and type _____<(OUD, etc)>

☐ **Groups**

<List them here> _____

☐ **Attributes**

<List them here> _____

☐ **Other** <Fully Describe> _____

Provisioning source

<How are the users provisioned>

☐ **SailPoint**

☐ **Other** <Fully Describe>_____

Service and Privileged Accounts

You Must Use CyberArk for Service and Privileged Accounts

<Privileged accounts needed with purpose, permissions and system.>

Number	Proposed Name	Description	Permissions

1		Domain LDAP Bind account(s)	Read all AD objects
2		Provisioning Account(s). Used to manage (i.e., create, modify, delete) user, contact and group objects	Create, modify and delete user, contact and group objects
3		Account for SQL access	Needs to be able to create and modify databases, database attribut database data.

6. Software

Name	Version	Date of release	Is this the latest GA version	If not, what is the latest GA Version
App1	8.0		No	10.0

7. Data

7.1 Data Flow Diagram

<Includes all data flows inside as well as to and from the system to outside sources>

7.2 Data that cannot exist in your system

☐ **FTI**

☐ **PCI**

☐ **PII**

☐ **Other**

---

8. Integration Patterns for other applications to consume your application

<This section calls out the integration patterns will utilize for other application to consume (what you publish to other applications). Can be API's or protocols that you publish so that others can easily integrate with you.>

9.Systems Dependent on Your Application

<This section calls out which systems are expected to consume your application>

10. Integrations

<This section calls out the Approved Integration method for integration with Enterprise Services you consume. This section will be updated with additional patterns as they are approved>

☐ **I am working with each Integration teams and have their approval of the below approaches**

MSI Key Stone Edge (KSE)

☐ **REST Push / Pull** – Tower systems will push new records & updates to Keystone Edge™ and pull new records & updates as well.

☐ **Push-Ping-Pull** – To avoid polling KSE, The Push/Pull refers to REST webservice invocations by the STS while the Ping refers to KSE email notification when a ticket updates. When KSE Ticket update occurs, an email notification to the STS is sent to trigger a PULL web service call to fetch the ticket changes.

☐ **Using Existing path for the Tower**

☐ **Other Approach** – Please describe below the approach that has been approved for only your system:

_____

MSS McAfee Security Information and Event Management (SIEM)

☐ **Other Approach** _____

MSI Digital Fuel (ITFM)

<This is how the billing information gets back to VITA>

☐ **Other Approach** _____

☐ **Not Needed – Give reason below**

_____

MSI CyberArk

<This is how the privileged user passwords and access is captured>

☐ **Agent Based**

☐ **API**

☐ **COV Vaulting**

☐ **Other Approach** <describe on line below>

☐ **Not Applicable** <describe why on line below>

_____

MSI SailPoint

<This is how the provisioning of users is done>

☐ **Other Approach** _____

SSDC OKTA – required if web based

☐ **SAML**

- ☐ **OAUTH**
- ☐ **Not Applicable**
- ☐ **Other Approach** _____

SSDC Active Directory

<This is the preferred identity source>

Instance:

- ☐ **COV**
- ☐ **AUTH**
- ☐ **Other** _____

Protocol:

- ☐ **Active Directory Kerberos**
- ☐ **Secure LDAP**
- ☐ **Other Approach** _____

EUC SCCM – deploys software to desktops

- ☐ **SCCM**
- ☐ **Not Applicable**
- ☐ **Other Approach** _____

SSDC SCCM – deploys software to servers

- ☐ **SCCM**
- ☐ **Not Applicable**
- ☐ **Other Approach** _____

Other Enterprise Service(s) you must integrate with

<List them here with the agreed on approach for integration to that service>

11. Business Services Mapping

Consume

<This is the listing of all the VAR's your architecture consumes>

Number	Name	Description
770	Unisys - Private Cloud High-level Design	How the Virtual Infrastructure is setup

Publish

<This is the listing of all consumable services that this architecture publishes>

Consumable Service Title	Description of Consumable Service
Spider	Brokers calls with other systems

12. Related Documents

SSP: <Document Name and submission date>

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved**

ECOS: <Document Name and submission date > - Only needed if there is a Cloud aspect to your service

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved** ☐ **Not Cloud Based - NA**

Any Exceptions you need: <Document Name(s) and submission date > <One line per exception>

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved** ☐ **Not Needed**

Disaster Recovery Plan: <Document Name and submission date >

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved**

New Hardening Standard(s) for your Service: <Document Name(s) and submission date >

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved** <One line per standard>

Integration Pattern(s) for your Service: <Document Name(s) and submission date > How does another system integrate with yours? <One line per pattern>

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved** ☐ **Not Needed – No integrations**

Archer: <Application ID(s) and submission date>

Status: ☐ **Not Started** ☐ **In Process** ☐ **In Review** ☐ **Approved**

13. Appendix

<Any additional information that you want to add that you feel is helpful>

References

<Any web sites references you feel would help answer questions>

Good Information - https://www.google.com

Terms and Acronyms

<this is where your acronyms go>

Item	Description
Configuration Management System (CMS)	Configuration Management System is a set of tools, data, and information that is used to support Service Asset and Configuration Management process
Continual Service Improvement (CSI)	A stage in the lifecycle of a service. Continual service improvement ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services and IT infrastructure in order to increase efficiency, effectiveness and cost effectiveness. Continual service improvement includes the seven-step improvement process. Although this process is associated with continual service improvement, most processes have activities that take place across multiple stages of the service lifecycle.

Item	Description
Critical Success Factor (CSF)	Something that must happen if an IT service, process, plan, project or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor.
Design Coordination (DEMC)	This is the abbreviation for the Design Coordination process
Information Technology Integrated Services Platform (ITISP)	All the hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support applications and IT services.
Key Performance Metric (KPI)	A metric that is used to help manage an IT services, process, plan, project or other activity.
Master Service Agreement (MSA)	Legal Contract between Customer (VITA) and the Service Tower Suppliers to execute defined services for the Commonwealth of Virginia.
Multi-sourcing Service Integrator (MSI)	The Integrated Supplier who has entered into an agreement with VITA to serve as the Multi-sourcing Service Integrator as described in in Section 1.4 (Managed Environment) of the Agreement.
Request for Change (RFC)	A formal proposal for a change to be made.
Request For Solution (RFS)	This is the Online form that is used to capture a solution request
Rough Order of Magnitude Quote (ROM)	This is an estimate done to gauge the size and cost of a project
Science Applications International Corporation (SAIC)	The Integrated Supplier who has entered into an agreement with VITA to serve as the Multi-sourcing Service Integrator as described in in Section 1.4 (Managed Environment) of the Agreement.
Security Systems Plan (SSP)	This is the document that the state of Virginia requires to capture how a solution will meet the requirements of SEC 525.
Service Design Packages (SDP)	Document(s) defining all aspects of an IT service and its requirements through each stage of its lifecycle. A service design package is produced for each new IT service, major change or IT service retirement.
Service Improvement Plan (SIP)	This is the documented solution to or outcome of a CSI issue.
Service Knowledge Management System (SKMS)	The system responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time.

Item	Description
Service Management Manual (SMM)	Defined repository of all defined processes and supporting artifacts for execution of IT Service Management capability.
Service Tower Supplier (STS)	A provider of a Service Tower. One Integrated Supplier may provide more than one Service Tower, each under the applicable Description of Services.
Virginia Information Technologies Agency (VITA)	An agency of the Commonwealth of Virginia pursuant to Chapter 20.1 (§§2.2-2005 et seq.) of the Code of Virginia.